サイバーセキュリティお助け隊サービス基準

（1.2 版）

独立行政法人情報処理推進機構

令和５年　４月　７日

目次

第１章　総則

１　サイバーセキュリティお助け隊サービスのコンセプト・目的

サイバーセキュリティお助け隊サービス（以下「お助け隊サービス」という。）は，中小企業のサイバーセキュリティ対策を支援するための相談窓口，異常の監視，事案発生時の初動対応（駆付け支援等）及び簡易サイバー保険を含む各種サービスを，安価かつ効果的なワンパッケージで，確実に提供するものをいう。

本基準は，お助け隊サービスの内容を明確化し，当該サービスに関し独立行政法人情報処理推進機構（IPA）が「サイバーセキュリティお助け隊マーク」の使用を許諾するにあたり充足すべき基準を定めることで，幅広い中小企業において無理なくサイバーセキュリティ対策を導入・運用することを支援するとともに，サプライチェーン全体のセキュリティの底上げを図ることを目的とする。

２　定義

本基準における用語の定義は，次に定めるところによる。

（１）ネットワーク監視型

お助け隊サービスのうち，UTM（Unified Threat Management・統合脅威管理）等のネットワークセキュリティ監視装置を用いてユーザーのネットワーク通信の異常を監視する形態のものをいう。

少なくとも以下の機能を実装すること。

ア　外部からの不審アクセス等の脅威の検知

イ　内部からの不正通信等の検知

ウ　検知した脅威等の防御

ただし，端末監視型の仕組みの防御機能と組み合わせて提供する場合は，ネットワーク監視型における防御機能の実装は要件として求めない。

（２）端末監視型

お助け隊サービスのうち，EDR（Endpoint Detection and Response）等のエンドポイントセキュリティソフトウェアを用いてユーザーの端末内部の挙動の異常を監視する形態のものをいう。

少なくとも以下の機能を実装すること。

ア　端末を常時監視し，異常や不審な挙動の検知

イ　検知した異常等の防御（お助け隊サービスと連動して一体的に機能するその他の防御も含む）

ただし，ネットワーク監視型の仕組みの防御機能と組み合わせて提供する

場合は,端末監視型における防御機能の実装は要件として求めない。

（３）実施主体

お助け隊サービスに関する契約を中小企業と行う事業者又は再販協力会社を通じてお助け隊サービスを提供する事業者であり，お助け隊サービス審査登録機関への申請等を行う者をいう。

（４）再販協力会社

実施主体が提供するお助け隊サービスに関する契約を中小企業と行う事業者をいう。

（５）パートナー

お助け隊サービスを構成することを目的に，実施主体に製品（UTM 等），サービス（駆付け等），保険を提供する事業者をいう。

（６）チーム

実施主体（１者）とパートナー（複数者でも可）から構成される。

（７）サイバーセキュリティお助け隊マーク

本基準を充足するお助け隊サービスに対し使用を許諾することを目的としたマークをいう。同サービスに関わるチームに対し，IPA により本マークの使用許諾がなされる。具体的なマークの使用条件及び注意事項は，マーク使用ガイドラインに定める。

（８）審査登録機関

サイバーセキュリティお助け隊サービス審査登録機関基準に基づき IPA から委託され，実施主体からの申請に基づき本基準に関する適合性の審査・登録を行う機関

（９）オプションサービス

各事業者がお助け隊サービスの他に，追加して提供する付加的なサービスをいう。

第２章　お助け隊サービスの基準に関する事項

１　要件

お助け隊サービスは，次に掲げる全ての要件を満たすものであること。

（１）相談窓口

ユーザーからのお助け隊サービスに関する次に掲げる全ての問合せを受け付ける窓口が一元的に設置又は案内されていること。

ア　お助け隊サービスの内容，価格，及び申込方法等に関する問合せ

イ　UTM の設置方法等，契約後にお助け隊サービスを導入する際の問合せ

ウ　アラートの解釈等，サービス利用中の技術的な問合せ

エ　価格調整等の営業的な問合せ

（２）異常の監視の仕組み

次のいずれかを含む異常監視サービスを提供すること。

ア　ユーザーのネットワークを 24 時間見守り，攻撃を検知・通知する仕組み（UTM 等のツールと異常監視サービスから構成）（ネットワーク監視型の場合）

イ　ユーザーの端末（PC やサーバ）を 24 時間見守り，攻撃を検知・通知する仕組み（EDR 等のツールと異常監視サービスから構成）（端末監視型の場合）

なお，いずれの異常監視サービスであっても検知した異常に応じ，セキュリティ上重大なインシデントの場合は，即時（60 分以内を目標），防御機能により十分な対策を行ったインシデント，あるいはインシデント対応が不要なアラートについては，後日のレポート（週 1 回）等によりユーザーに通知すること。

（３）緊急時の対応支援

ユーザーと合意したサービス規約等に基づき，ユーザーから要請された場合，ユーザーの指定する場所に技術者を派遣（駆付け支援）し，緊急時の対応支援を行うこと（ユーザーからの合意を得て、リモートによる対応支援も可とする）。また，緊急時の対応支援は，簡易サイバー保険を活用する場合を含めて，異常の監視の仕組みの導入に伴う初期対応に必要な駆付け支援を除き，少なくとも年１回はユーザーの自己負担が生じないようにすること。ただし，駆付け支援を行うための移動に要する交通費などの諸経費は除くことができる。

（４）中小企業でも導入・運用できる簡単さ

IT やセキュリティの専門知識のないユーザーでも導入・運用できるような工夫が凝らされていること。

（５）簡易サイバー保険

インシデント対応時に突発的に発生する各種コストを補償するサイバー保険が付帯されていること。なお，サイバー保険の補償範囲（補償対象となる事項，補償回数，補償限度額，免責金額等）及びユーザーにおいて自己負担が生じる場合，サービス規約等に記載するとともに，別途ユーザーにとって分かりやすい説明資料を用意すること。

（６）上記機能のワンパッケージ提供

原則として（１）～（５）の機能をユーザーが個別に契約することなく，一元的に契約可能であること。ただし，法令等やむを得ない事情がある場

合は個別契約も可とするものの，その場合にあってはユーザーにおいて手続上の煩雑さを伴わないよう工夫が凝らされていること。また，異常の監視装置の製造メーカー・型式，サービス提供の所在国及び把握している場合はデータ保存先の所在国についてサービス規約等に記載すること。

（７）中小企業でも導入・維持できる価格等

前項の規定によりワンパッケージで提供されるお助け隊サービスについて，以下のアからオ全てを満たすこと。

ア　お助け隊サービスの合計価格が月額１万円以下（税抜き）に相当する価格であること（ネットワーク監視型の場合），又は端末１台あたり月額 2,000 円以下（税抜き）に相当する価格であること（端末監視型の場合）。これらの仕組みを合わせて提供する場合には，この和（月額１万円に端末１台あたり月額 2,000 円を加えた価格（税抜き））に相当する価格を超えない価格であること。なお，いずれも端末１台から契約可能とすること。

イ　最低契約年数は２年以内であること。

ウ　初期費用，契約年数等の契約にかかる条件をサービス規約等に記載するとともに，口頭又は書面によりユーザーに分かりやすく説明すること。

エ　初期費用の金額は，幅広い中小企業において無理なく導入可能な価格であることが望ましいため，必要な場合であっても，最大で以下の金額を上回らないこと。

ネットワーク監視型の場合・・　50 万円以下（税抜き）

端末監視型の場合・・　端末数によらず 50 万円以下（税抜き）

併用型の場合・・　これらの和に相当する価格（100 万円（税抜き））を超えない価格であること。

オ　途中解約した場合の違約金やユーザー側の契約解除の権利等をサービス規約等に記載するとともに，口頭又は書面によりユーザーに分かりやすく説明すること。

（８）中小企業向けセキュリティサービス提供実績

IPA 実施事業「中小企業向けサイバーセキュリティ事後対応支援実証事業」，若しくは「令和２年度中小企業向けサイバーセキュリティ対策支援体制構築事業」に参加していたこと，又は類似のサービスを中小企業向けに提供・運用した実績があること。

（９）情報共有

IPA からの要請に応じて，お助け隊サービス事業者間等の情報共有に協力することに合意し，少なくともアラートの統計情報の提供に応じること。なお，IPA は，本項に基づき情報共有を求めるにあたっては，その内容や

方法について，別にガイドライン等を定めることとする。

(10) 事業継続性

お助け隊サービスの提供に必要な要員の確保，品質管理等の社内プロセス整備，企業としての安定した財政基盤，経理処理能力等を有し，それらを審査登録機関に対して示せること。なお，お助け隊サービスの提供が困難となる事情が生じた場合，その他必要な場合には，IPA 及び審査登録機関に対しその旨速やかに報告を行うこと。また,再販協力会社によるお助け隊サービスの提供が困難となる場合は,実施主体がその責任を負うこと。

(11) サービス基準の遵守

実施主体は，日本の法令及び本基準が定める事項を遵守すること。

２　更新・その他

（１）登録の更新

実施主体は，本基準の適合性に関し２年毎に更新審査を受けること。

（２）サービス内容の変更

実施主体は，お助け隊サービスの提供内容に変更が生じた場合は，IPA が別に定めるガイドライン等に従い，速やかに届け出ること。ただし，変更内容によっては改めて申請を要する場合があるが，これに従うこと。

（３）サービスの取消し

再販協力会社も含め本基準に逸脱した場合，又はその強い疑いがあり，お助け隊サービス制度に対する社会的信頼保持等の観点から必要と考えられる場合，IPA は実施主体に対し是正のために必要な措置を講ずべきことを指示することができる。この場合，相当の期間を定めて是正のための機会を与えるが，是正に応じない際には，IPA はそのサービスのかかる登録を取り消す場合がある。

（４）審査登録機関への協力

チームは，本基準の適合性にかかるサーベイランスをはじめ，審査登録機関からの協力要請等があった場合には，誠実にこれに対応すること。

附則

１　推奨事項

中小企業におけるサイバーセキュリティ対策の導入・運用の更なる利便性向上を図る趣旨のもと，お助け隊サービスの提供にあたっては以下の事項が推奨されるものである。

（１）独自のオプションサービス提供

お助け隊サービスの他に，さらなるセキュリティ対策の導入を考える企業のためのオプションサービスを用意すること

例：・事前アセスメント等の簡易コンサルティングサービス
・ネットワーク監視の仕組み
・デジタルフォレンジック等より広い範囲のコストを補償するサイバー保険

（２）日本発の技術・製品の活用

日本特有のサイバー攻撃動向に対してより高精度で対応するため，日本発の技術やそれを用いた製品・サービスを活用すること

（３）ネットワーク監視型のサービスの提供

ネットワーク監視型のサービスを提供する場合，ネットワーク通信全体を監視できるよう監視機器の設置する場所等を考慮すること。

（４）端末監視型のサービスの提供

端末監視型のサービスを提供する場合，少なくとも重要情報を取り扱う端末には導入すること。

２　その他

IPA は，本基準第１章１．の目的に照らし必要に応じて本基準の内容について検討を加え，その結果に基づいて適宜見直しを行うこととする。